DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR COMBAT COMMAND
LANGLEY AIR FORCE BASE, VIRGINIA

28 Sep 04

MEMORANDUM FOR HQ ACC/DRS

FROM: HQ ACC/SCT

SUBJECT: Extension of ACC Interim Certificate to Operate (CtO) and Interim Approval to Operate (IATO) for Portable Flight Planning System (PFPS) Version 3.2

1. In accordance with AFPD 33-2, *Information Protection* and ACCI 33-174, *Certifying the ACC Enterprise*, I approve the extended operation of the Portable Flight Planning System (PFPS) version 3.2 until 6 Oct 05 and extend both the ICtO and IATO. This approval allows the system to operate at all ACC bases up to the SECRET level in the system high security mode of operation in accordance with the attached HQ ACC/SCSC memorandum (Atch 1). The Designated Approving Authority's (DAA) review of the Systems Security Authorization Agreement (SSAA) verifies that some system security countermeasures have been implemented, and an acceptable level-of-protection exists.

2. The assigned Information Systems Security Officer (ISSO) is required to follow the SSAA and DAA provided guidance throughout the life cycle of the system. The ACC Network Operations and Security Center will inform the local Network Control Center that the system is authorized for use on the ACC Enterprise. Before system activation, the functional information system's owner and the host wing Information Assurance Office will complete the ACC Site Certification Checklist. The ISSO maintains the completed checklist and SSAA for the system's life cycle.

3. An automatic or cursory extension of an Accreditation will not be given beyond the expiration date of this approval. During this period, you must ensure appropriate actions are taken to address residual risks identified. Failure to mitigate the risks may prohibit use of the application beyond the date of this approval. An ACC/SCS Information Technology (IT) consultant will continue to work with your staff to develop a corrective action plan to resolve each of the remaining risks.

4. This CtO and Accreditation extension is only valid for the current version's system software configuration and associated hardware. Any changes to this system (i.e., revisions, upgrades, or new versions) will nullify this approval. Please contact your ACC/SCS IT consultant, SMSgt David Mitchell, HQ ACC/SCSO, DSN 574-7745, if you have any questions.

ROBERT B. JACK II, GS-15, DAF
Technical Director
Communications and Information Systems

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR COMBAT COMMAND
LANGLEY AIR FORCE BASE, VIRGINIA

24 Sep 2004

MEMORANDUM FOR HQ ACC/SCS

FROM: HQ ACC/SCSC

SUBJECT: Recommendation for an extension of the ACC Certificate to Operate (CtO) and Accreditation for Portable Flight Planning System (PFPS) version 3.2

1. PFPS 3.2 was re-accredited for an ICtO/IATO on 6 Oct 03 due to Windows XP upgrade. The next version (PFPS 3.3.1) is currently under testing and is not expected to field until Apr 2005, so we recommend a 1 year extension of the approval for PFPS 3.2 with no changes. PFPS normally consists of a single ground-based, integrated, single-user, deployable mission planning system that interfaces with aircraft systems. PFPS will be used by aircraft mission planners throughout ACC. PFPS 3.2 operates as a single stand-alone PC or may connect to a LAN for access to other systems' data. After review and evaluation of the certification package, we recommend an extension of the existing ICtO and IATO for PFPS 3.2 in the system high security mode of operation up to the SECRET level. Anything above the collateral SECRET level must be approved appropriately.

2. Areas of residual risk remain; which require additional risk management measures. All remaining risks can be grouped into three main categories, summarized below. A detailed breakdown of residual risk is attached.

a. Risks with No Countermeasures: These are all the risks without any realistic countermeasures available. There may be certain limitations and constraints imposed to help mitigate these risks to an acceptable level.

b. Risks with Insufficient Countermeasures: These are all the risks with countermeasures applied, however, the countermeasures do not fully mitigate the risk. Countermeasures to further reduce risk may be unavailable or not economically feasible.

c. Mitigated Risks: These risks are deemed to have been reduced to a level where they no longer pose a measurable risk to system operation. They were presented as risks in the system certification package (identified during the risk analysis process or security test and evaluation), however, applied countermeasures or imposed limitations and constraints nullify these risks.

TRACY A. BOBO, Maj, USAF
Acting Chief, IT Assessment Branch
Directorate, Communications and Information Systems

Attachment:
Detailed Risk Breakdown

Global Power For America

Detailed Risk Breakdown
for
Portable Flight Planning System 3.2

1. Risks with No Countermeasures:

a. Risk: Incomplete SSAA

(1) Impact: An interim approval can be given based on a review of available documentation

(2) Corrective Measure(s): Complete the SSAA to include appropriate appendices

(3) Limiting Factors:

i) The Risk Analysis documents the residual risk of the system after taking into account the results of the ST&E. The Trusted Facility Manual (TFM) provides the system administrator with instructions on how to securely run the system. The Security Features Users Guide (SFUG) instructs all users in the security features of the system. The RA, TFM, and SFUG are needed to ensure that the system operates securely.

ii) The next version of PFPS (3.3.1) will have a complete SSAA

(4) Recommendation: Acceptable for extension of CtO and Accreditation.

2. Risks with Insufficient Countermeasures:

a. Risk: The commercial-off-the-shelf (COTS) products were developed in an open environment without integrity features.

(1) Impact: There is the potential that system programmers may have inserted malicious code or macros during system development. Also, the systems may be altered during normal processing by a malicious user.

(2) Corrective Measure: Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the trusted computer base. The system should be designed with system integrity functionality, such as check sums.

(3) Recommendation: Acceptable for extension.

b. Risk: Accreditation Boundary is not clearly defined

(1) Impact: Clear lines of responsibility must be documented to ensure responsibility is in tact for the system and any network(s) interfaced. The responsible person or organization must be clearly defined for each component, connection, interface, etc.

(2) Corrective Measure: Complete the SSAA to include a thorough architectural description and diagram of PFPS indicating interfaces with any other system(s) that clearly delineates the accreditation boundary.

(3) Limiting Factor: PFPS is based on a legacy system with roles and responsibilities existing for almost 10 years. Also this request and recommendation do not include any system interfaces yet.

(4) Recommendation: Acceptable for interim based on legacy status and no new introduction of risk to the enterprise network.

c. Risk: The System Security Policy (section 3.5) contains the statement: "System-level documentation not originally required by contract for a network component shall not be requested after the fact"

(1) Impact: The SSAA is intended as a living document, changeable with software/hardware changes. The DAA does not forfeit the right to request documentation as needed.

(2) Corrective Measure: Remove this statement from any/all SSAA documentation.

(3) Recommendation: Acceptable for this limited approval period

d. Risk: References throughout documentation indicate SAR (Special Access Required) classified data. ACC/SC is limited in scope to Top Secret Collateral and below.

(1) Impact: SAR must be approved through SAF/AQ.

(2) Corrective Measure: Include a copy of the SAF/AQ approval as an appendix to the SSAA.

(3) Limiting Factor: The ACC/SC approval letter specifies collateral only; it is understood that SAF/AQ has/will approve any SAR use before it goes operational. Section 2.2, page 6 of the Security CONOPS says, "It is recognized that there are locations where PFPS will b operating at the TS/SAR level. These locations will need to obtain an accreditation from their appropriate DAA."

(4) Recommendation: Acceptable

e. Risk: Use of "periods processing" to handle multiple classifications of data

(1) Impact: Potential of creating security incident(s) if a network is accessed by a mismatched classification. Temporary denial of service situation if LAN has to be sanitized.

(2) Corrective Measure: A DSAWG (DISN Security Accreditation Working Group) approved SABI Solution (Trusted Guard(s)) would mitigate this risk, but that is not feasible because it would be prohibitively expensive. The hardware separation is the only affordable mitigation.

(3) Limiting Factor: The SSAA including the Security Policy gives clear direction about how to process different classification levels and how to change from one to another by switching hard drives. If proper procedure is used, there is no direct or indirect interface from one classification to another.

(4) Recommendation: Acceptable

3. Mitigated Risks:

a. Risk: The physical security o f the base network will depend largely on the site-specific security procedures in pace on the base.

(1) Impact: Improper security procedures will allow an individual access to the hardware components, which will allow that individual to bypass audit procedures and possibly deny service to the users or compromise the confidentiality and integrity of the data.

(2) Corrective Measure: Site specific procedures must be approved by the local Certifying Authority's representative

(3) Recommendation: Acceptable

b. Risk: Potential of a security incident due to the failure to maintain a secure system configuration.

(1) Impact: Potential for loss of assurance in data integrity, confidentiality, and availability

(2) Corrective Measure: The ISSO should monitor CERT and AFCERT advisories for published problems with system hardware and software. Advisories with patches that are published by AFCERT should be added to the system.

(3) Recommendation: Acceptable

c. Risk: The Security CONOPS, sections 3.3.1 and 3.3.2 (Personnel and Physical Security respectively), page 16 says "Each MAJCOM will be responsible..." The CONOPS should direct users in these areas based on DOD-wide regulations and policy; this is not varied by MAJCOM.

(1) Impact: The Security CONOPS does not serve the end users as a document that stands on its own. It will consume extra time to be repeatedly completed when it should be delivered in a usable form.

(2) Corrective Measure: Complete these sections of the Security CONOPS

(3) Limiting Factor: Other sections of the SSAA direct clearance requirements and minimum physical security standards for the varying classifications for which PFPS can be used.

(4) Recommendation: Acceptable for an interim period

SITE CERTIFICATION CHECKLIST

PFPS 3.2

	Completed	N/A
Site Security Personnel		
1. Identify Local Certification Authority.		
2. Notify Wing Information Assurance Office of impending installation.		
3. Assign other system security officials, (i.e. ISSO, SA, FSA, ...) and document in writing.		
Documentation		
1. Ensure local personnel possess a copy of the Certificate to Operate (CtO) package to include SSAA, DAA letter, and Breakdown of Residual Risks.		
2. Install AIS or application as described in the CtO package.		
3. Document a list of all hardware variances. If there are variances do not implement until a change request is validated by the Certifying Authority and approved by MAJCOM DAA		
4. Document a list of all software variances. If there are variances, do not implement until a change request is validated by the Certifying Authority and is approved by MAJCOM DAA		
5. Include a diagram of the system network if adding systems. Submit diagram with completed checklist.		
6. Document any site-specific security policies that are not already in the System Security Policy. If there are changes to the security policies do not implement until a change request is validated by the Certifying Authority and approved by MAJCOM DAA.		
7. Document any site-specific additions/deletions to the Threat/Vulnerability Matrix.		
Certification		
1. Perform any countermeasures identified in Risk Analysis section of SSAA and ACC Breakdown of Residual Risk.		
2. Verify system integrity by running an ISS scan. Correct and identify any additional vulnerabilities.		
3. If the AIS connects two or more different security classification networks, it must use an approved Secret and Below Interoperability (SABI) solution and receive final SABI board approval before operational use.		
4. Return this completed checklist to SCS.		
Software Licensing		
1. Ensure unit ISSO maintains a locatable copy of software license agreement per seat		
2. Ensure ISSO monitors compliance with the software license agreement		

Certification Authority's Validation

Date Submitted: _____

Signature: _____

Name: _____

Title: _____